6.   THE CLAIMS

It is claimed:

1. A method of displaying network data comprising:

    a) entering a request for the network data into a computer;

5   b) creating a network data request;

    c) transmitting the network data request from the computer to a server;

    d) verifying the network data request by comparing the network data request to

    criteria defined by a business rule;

    e) obtaining the network data;

10 f) creating a data response;

    g) transmitting the data response from the server to the computer; and

    h) displaying the network data.

2. The method of claim 1, wherein the request for the network data is entered into a

15 browser running on the computer.

3. The method of claim 1, wherein the act of entering a request for network data

includes entering a request for network data that includes the name of a gateway server.

20 4. The method of claim 1, wherein the act of entering a request for network data

includes entering a request for network data that includes the name of a monitoring

server.

5. The method of claim 1, wherein the act of transmitting the network data request includes transmitting a network data request that has been encrypted.

6. The method of claim 1, wherein the act of transmitting the network data request

5   includes transmitting a network data request that has been encrypted via a first private key.

7. The method of claim 1, wherein the act of transmitting the network data request includes transmitting a network data request that has been encrypted via a first private

10   key and a second private key.

8. The method of claim 1, wherein the act of verifying the network data request includes comparing the requested network data to criteria defined by a business rule.

15   9. The method of claim 1, wherein the act of verifying the network data request includes comparing a user ID to criteria defined by a business rule.

10. The method of claim 1, wherein the act of verifying the network data request includes comparing the organization of a user to criteria defined by a business rule.

20

11. The method of claim 1, wherein the act of verifying the network data request includes comparing a user password to criteria defined by a business rule.

12. The method of claim 1, wherein the act of verifying the network data request includes comparing information that identifies the computer to criteria defined by a business rule.

13. The method of claim 1, wherein the act of displaying the network data includes displaying the network data on a browser running on the computer.

14. A method of displaying network data comprising:

   a) entering a request for the network data into a computer;

   b) creating a first network data request;

   c) transmitting the first network data request from the computer to a first server;

   d) verifying the first network data request

   e) creating a second network data request;

   f) transmitting the second network data request from the first server to a second server;

   g) verifying the second network data request;

   h) obtaining the network data;

   i) creating a first data response;

   j) transmitting the first data response from the second server to the first server;

   k) verifying the first data response;

   l) creating a second data response;

   m) verifying the second data response;

   n) transmitting the second data response from the first server to the computer; and

o) displaying the network data.

15. The method of claim 14, wherein the request for the network data is entered into a browser running on the computer.

5

16. The method of claim 14, wherein the act of entering a request for network data includes entering a request for network data that includes the name of a gateway server.

17. The method of claim 14, wherein the act of entering a request for network data

10 includes entering a request for network data that includes the name of a monitoring server.

18. The method of claim 14, wherein the act of transmitting the second network data request includes transmitting a network data request that has been encrypted.

15

19. The method of claim 14, wherein the act of transmitting the second network data request includes transmitting a network data request that has been encrypted via a first private key.

20 20. The method of claim 14, wherein the act of transmitting the second network data request includes transmitting a network data request that has been encrypted via a first private key and a second private key.

21. The method of claim 14, wherein the act of verifying the second network data request includes comparing the requested network data to criteria defined by a business rule.

22. The method of claim 14, wherein the act of verifying the second network data request

5   includes comparing a user ID to criteria defined by a business rule.

23. The method of claim 14, wherein the act of verifying the second network data request includes comparing the organization of a user to criteria defined by a business rule.

10   24. The method of claim 14, wherein the act of verifying the second network data request includes comparing a user password to criteria defined by a business rule.

25. The method of claim 14, wherein the act of verifying the second network data request includes comparing information that identifies the computer to criteria defined by a

15   business rule.

26. The method of claim 14, wherein the act of verifying the second network data request includes comparing information that identifies the first server to criteria defined by a business rule.

20

27. The method of claim 14, wherein the act of displaying the network data includes displaying the network data on a browser running on the computer.

28. A program storage device that contains computer readable instructions that when executed by a server perform the following:

    a) verify a network data request by comparing the network data request to criteria defined by a business rule;

    b) obtain network data;

    c) create a data response; and

    d) transmit the data response from the server to a computer.

29. A method of verifying the authenticity of software comprising:

    a) based upon the software, generating a text string;

    b) based upon the text string, generating a first hash value; and

    c) comparing the first hash value with a second hash value.

30. The method of claim 29, wherein the act of generating a text string includes generating a text string based upon the name of a software file.

31. The method of claim 29, wherein the act of generating a text string includes generating a text string based upon the date of a software file.

32. The method of claim 29, wherein the act of generating a text string includes generating a text string based upon the directory of a software file.

33. The method of claim 29, wherein the act of generating a text string includes generating a text string based upon the size of a software file.

34. The method of claim 29, wherein the act of comparing the first hash value with a second hash value includes comparing the first hash value with a second hash value that was included on a program storage device that includes the software.

35. The method of claim 29, wherein the act of comparing the first hash value with a second hash value includes comparing the first hash value with a second hash value that was provided via the Internet.

36. The method of claim 29, wherein the act of comparing the first hash value with a second hash value includes comparing the first hash value with a second hash value that was provided via a facsimile.

37. The method of claim 29, wherein the act of comparing the first hash value with a second hash value includes comparing the first hash value with a second hash value that was provided via a telephone call.

38. The method of claim 29, wherein the act of comparing the first hash value with a second hash value includes comparing the first hash value with a second hash value that was provided via an email.

5   39. The method of claim 29, wherein the act of comparing the first hash value with a second hash value includes comparing the first hash value with a second hash value that was provided via a written document.